

僵尸网络扎根互联网 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/251/2021_2022__E5_83_B5_E5_B0_B8_E7_BD_91_E7_c101_251129.htm 由受攻击的个人电脑组成的网络被称之为“僵尸网络”（botnet）正扎根于中国的宽带网络中，影响着中国五分之一的台式电脑系统，威胁着政府、金融机构以及其他行业的计算机安全。这不是危言耸听。来自全球著名反病毒软件商赛门铁克公司日前发布的《第10期互联网安全威胁报告》显示，根据今年上半年监测的数据，中国拥有的“僵尸网络”电脑数目最多，全世界共有470万台，而中国就占到了近20%。黑客们正受益于国内互联网用户数连续增长的乾坤盛世。据CNNIC的统计用户数已达9400万，在庞大的用户群中能轻松捕获那些疏于防范的用户群，一台自诞生起就没打过补丁的PC机弹指间成了危害网络安全的帮凶，而主人们正坐在屏幕前与他人神聊，丝毫不知自己在黑客眼中已与裸体无异。所谓“僵尸网络”，就是黑客利用“僵尸程序”控制大量互联网用户的计算机，这些计算机就像“僵尸”一样被黑客所操纵。随时按照黑客的指令展开DoS攻击或发送垃圾信息，而真正的用户却毫不知情，就仿佛没有自主意识的僵尸一般。成千上万台被感染的计算机组成的僵尸军团，可以在统一号令下同时对网络的某个节点发动攻击，从而具备攻城拔寨的强大破坏力，成为一支网络上可以用于进行各种破坏活动的“僵尸***”。僵尸网络实际上是垃圾邮件、病毒和特洛伊木马发展的最终结果。这些自我复制的危险蠕虫在这一切的背后显然有犯罪组织在影响和操纵，通常作为网络恐怖（Cyberterrorist）或勒索攻击

的手段之一。不仅会使受害的目标网站和主要应用瘫痪，而且还会显著影响受害网站运营商的服务能力和性能。被黑客控制了电脑，被称为“肉鸡”，由许多“肉鸡”组成的计算机网络“僵尸网络”，它们被用来进行垃圾邮件发送的中继站、放置恶意网站或者发起DoS攻击敲诈企业。发起DoS攻击敲诈企业。由于多年来网络系统累积下了无数的漏洞，网络中潜伏的好事者会以此为缺口来对系统进行攻击。一些存在安全隐患的电脑系统很容易被黑客劫持，在这些电脑上开置后门。之所以“僵尸网络”成为当今网络安全五大威胁之一，主要是因为以下几点：一是攻击技术不复杂。黑客经常使用的方式之一是“DoS（拒绝服务）”攻击，利用一些网络通讯协议本身固有的缺陷，通过伪造超过服务器处理能力的请求数据，造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。就像一条路只能容许100人通过，黑客控制了100个木头人放在路上，其他人就不能通过了。DoS攻击并不是一种复杂的技术，具有初级安全知识的人就可以很容易策动和实施危害很大的攻击，但对其的追查却很困难，因而采用此种攻击方式的黑客手段非常隐蔽、娴熟。二是与谋取经济利益有关。在2005年底发布的“黑客被捕案例与网络诈骗事件”中，全球著名网络安全软件及服务提供商趋势科技发现，这些案件中的黑客已经不是像从前那样，要借助写病毒炫耀技术、扬名立万，而是几乎都与谋取经济利益有关。那些攻击网站、实施诈骗的黑客，首先要挑选出那些“值得攻击”的网站，“值得”的指标如人气旺、流量大、在业内具有一定知名度等；选定目标后，研究该网站的漏洞所在，制定攻击策略，发动攻击。目前“僵尸网络

”已经越来越多地被用作敲诈工具。如果是做“杀手”，费用也仅需每小时100美元。三是网站资金匮乏难以抵御。面对随时可能的黑客攻击，特别是中小网站需要加强防护，配置防火墙、黑洞及备份等重要软硬件防护设施，聘请专业的维护人员，以及增加带宽。但这意味着必须加大投入，而防范DoS攻击最为有效的硬件防火墙黑洞设备最便宜的一款低端百兆产品也要5万多元，资金之困，成为抵御黑客的首要难题。由于防范手段和资金的匮乏，造成了绝大多数托管网站被迫处于“不设防”的运行状态，一旦被攻击，就会导致整个网络瘫痪。四是被DoS攻击后难以追查。随着技术的进步，潜心研究DoS攻击的黑客也在不断开发新的程序，因此也更加难以追查。防火墙日志可发现被攻击的原因，但这仅仅是提供一个线索。被攻击的受损害者可到当地派出所报案，如派出所提出请求，网监处可进行配合调查，但一定要有相关证据才行。但这些证据保存在软件里，可以很容易被转移或毁灭。网络犯罪环境创造了一个“第五空间”（其他空间是指领陆、领水、领空和拟制领土），证据很难收集。五是网络犯罪的司法管辖权不确定。传统的刑事司法管辖一般都以某种相对稳定的时空联系作为基础，像固定住所等，而这些联系却很难体现在网络活动中。就目前的情况来看，尚没有任何国家能够单独制定出好的解决方案。要想彻底改变这种被动现状，仅靠反病毒厂商自身难以做到，它与国家的政策、网络环境的净化、客户的安全意识、网络文明都有关。黑客离人们的日常生活越来越近，一切似乎都是那么触目惊心。网络领域的“僵尸大军”正以平均每天超过17.3万台的速度快速扩容，尤其值得关注的是，随着国内互联网的飞速发展

，其中大约20%竟然来自中国，中国已经成为这一领域至关重要的战场。目前，在中**现的最大的一个“僵尸网络”控制着约10万台计算机，而境外曾经出现过40多万用户被“僵尸网络”控制的事件。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com